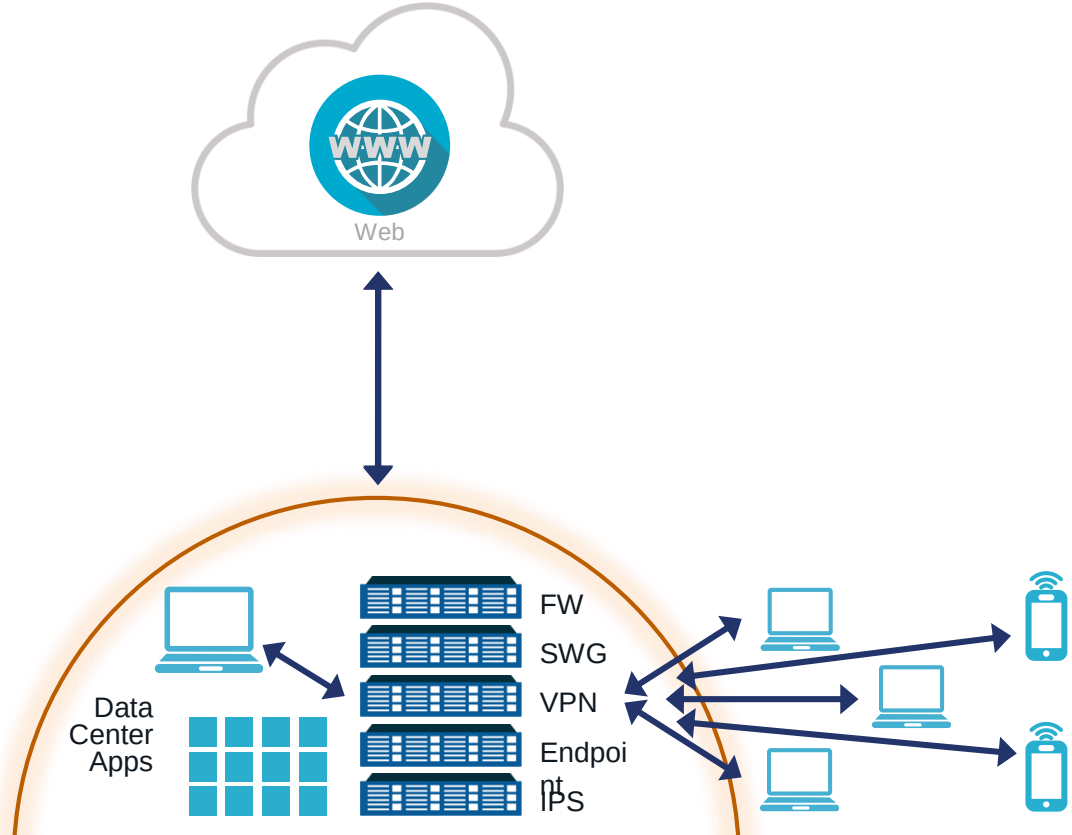
Cloud Security Today

Presenter: Jason Sheffield

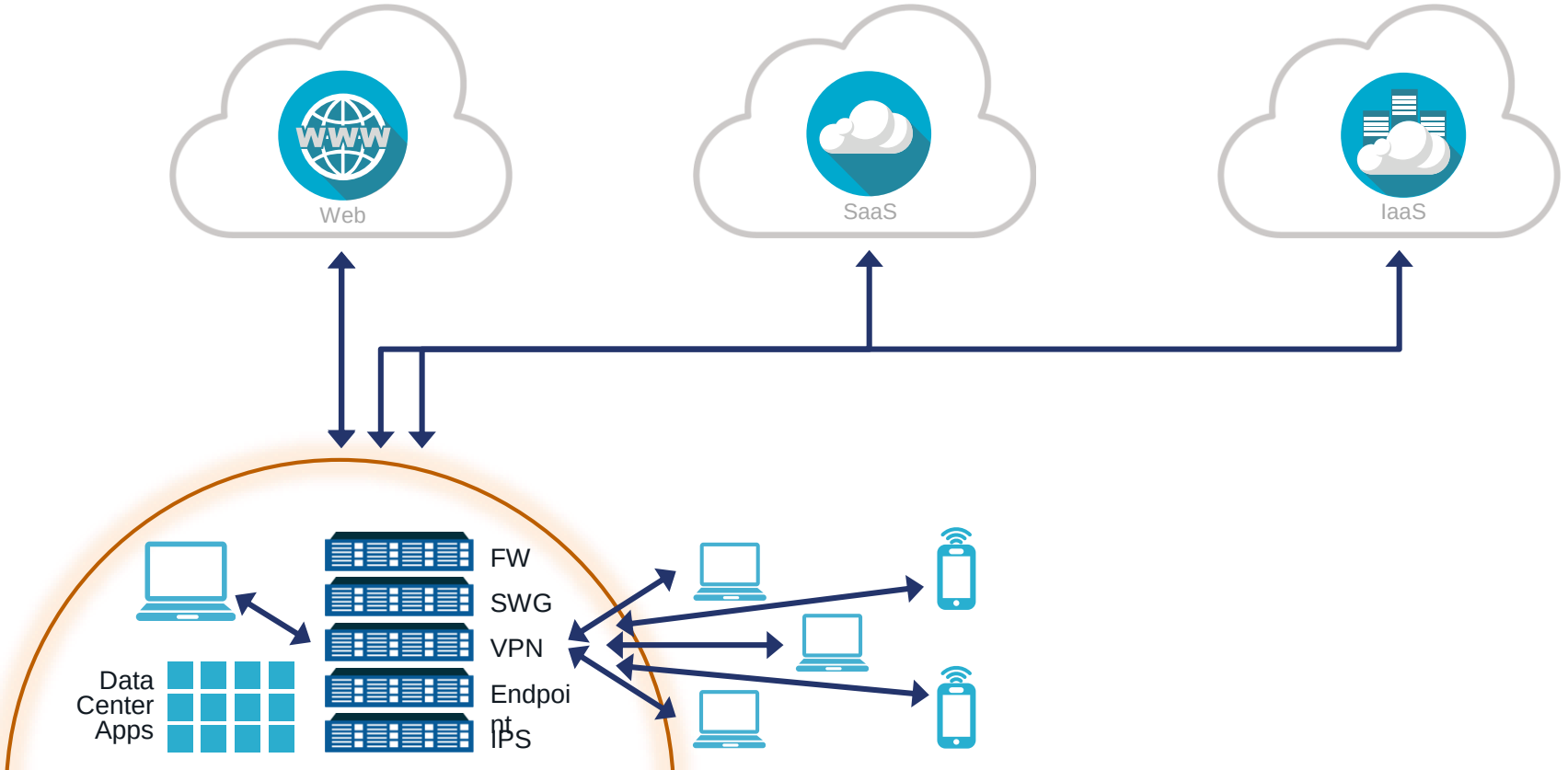
Topics

- What are the issues today?
- What is the Cloud?
- How the Cloud is delivered: Iaas, PaaS and SaaS
- Cloud security challenges and risk
- Current Cloud security report
- Cloud security technology drivers
- Common use cases for Cloud security technologies
- What technologies exist to address risk?

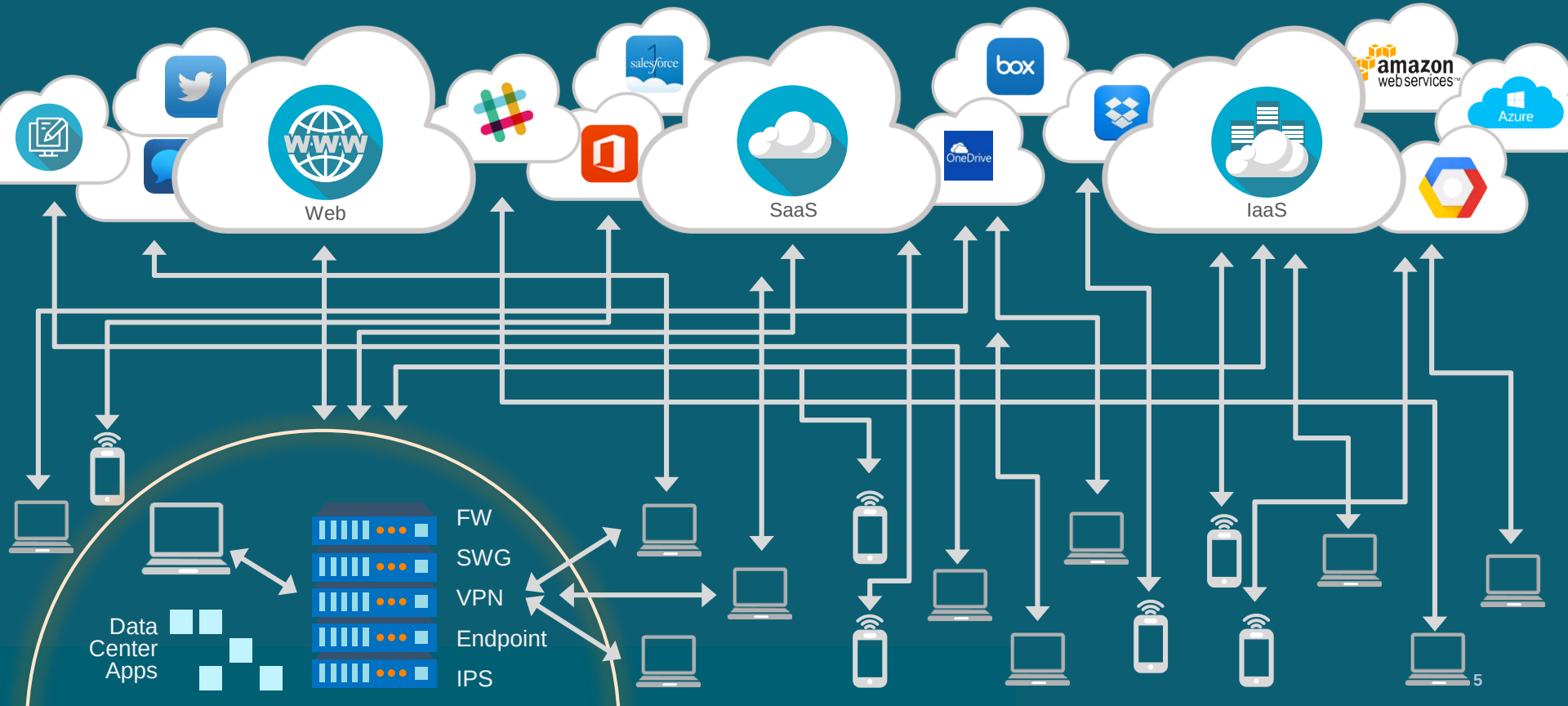
Old IT Security Architecture From Yesterday



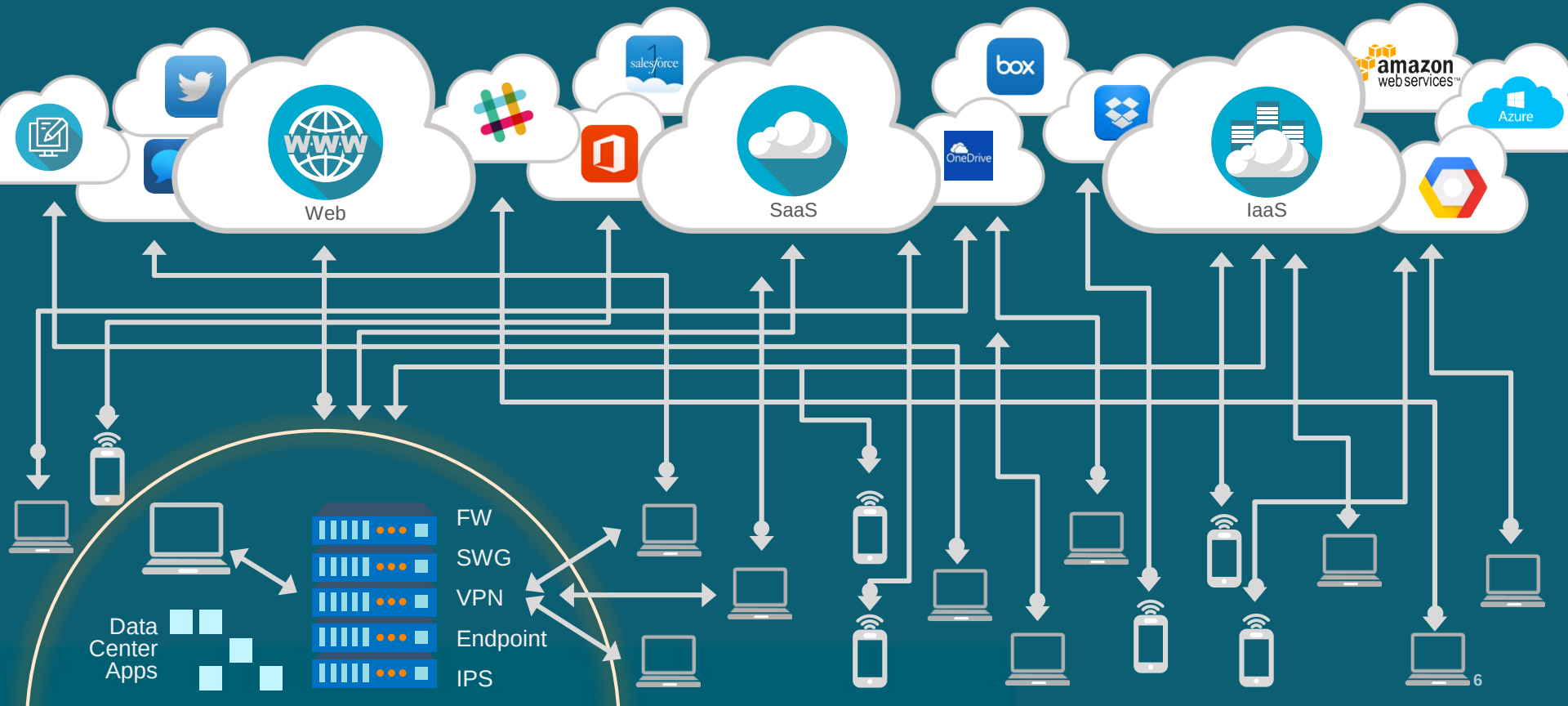
Old IT Security Architecture From Yesterday



With Digital Transformation … Everything Changed

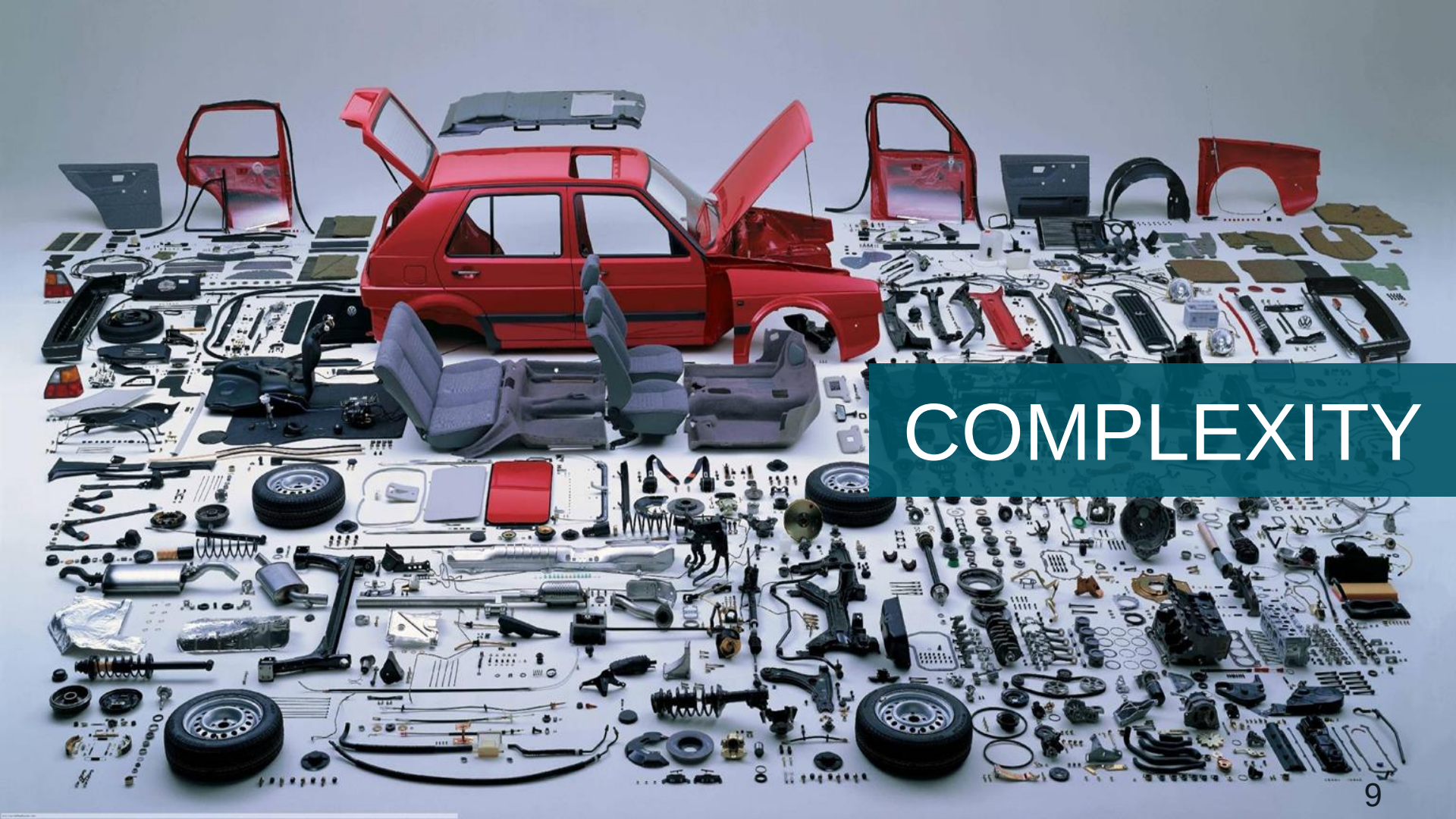


With Digital Transformation … Data is Everywhere

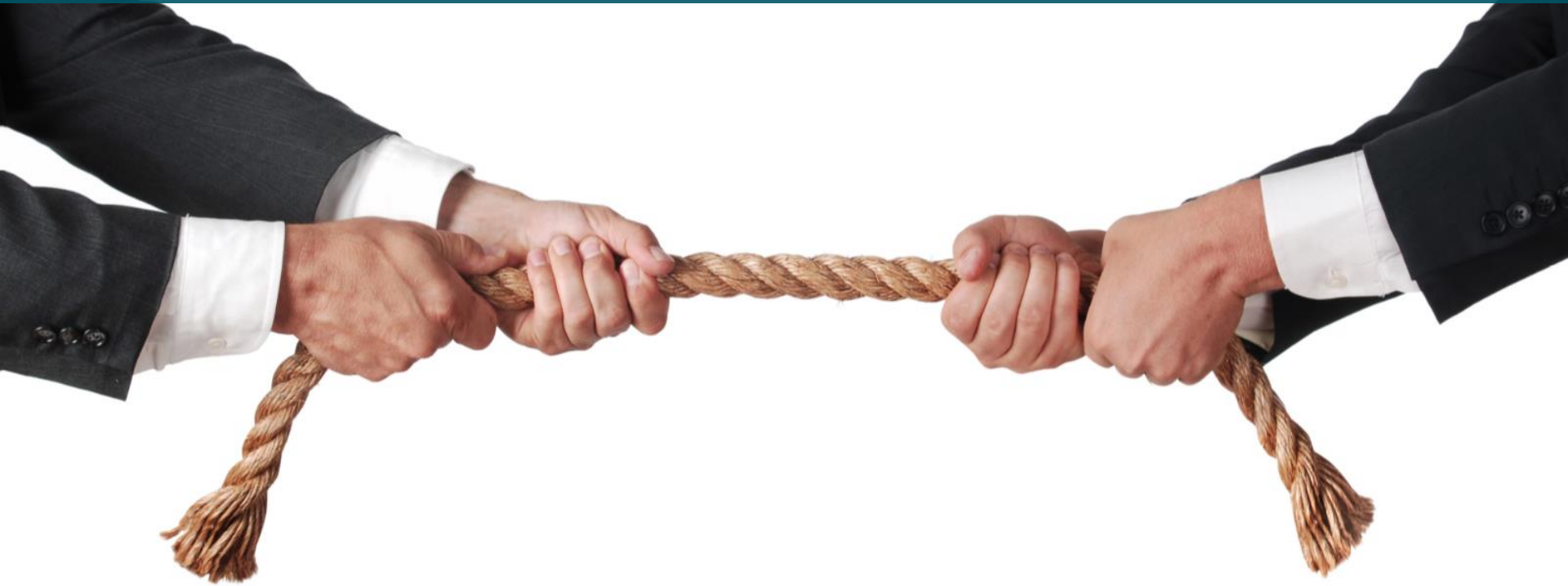



DATA
FLOWS
LIKE
WATER

LACK OF VISIBILITY


COMPLEXITY

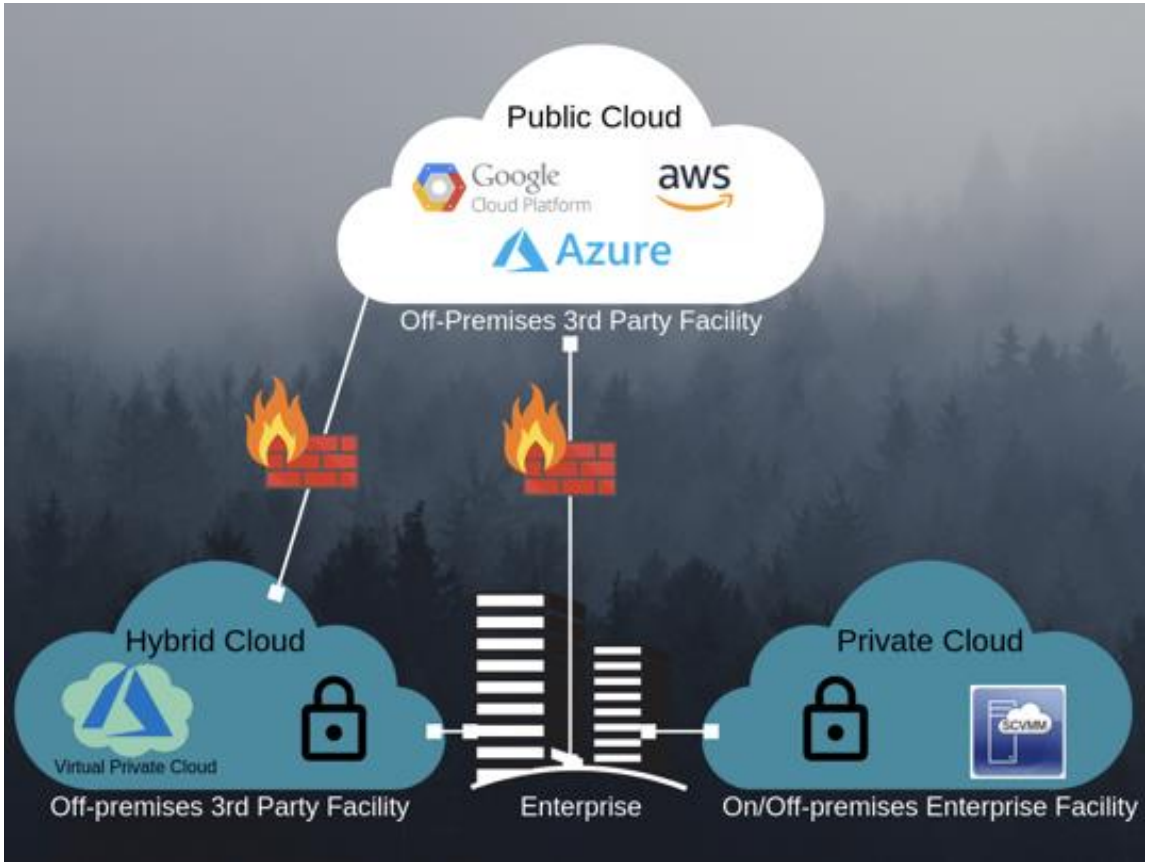
CONTROLS CREATES FRICTION



What is the Cloud?

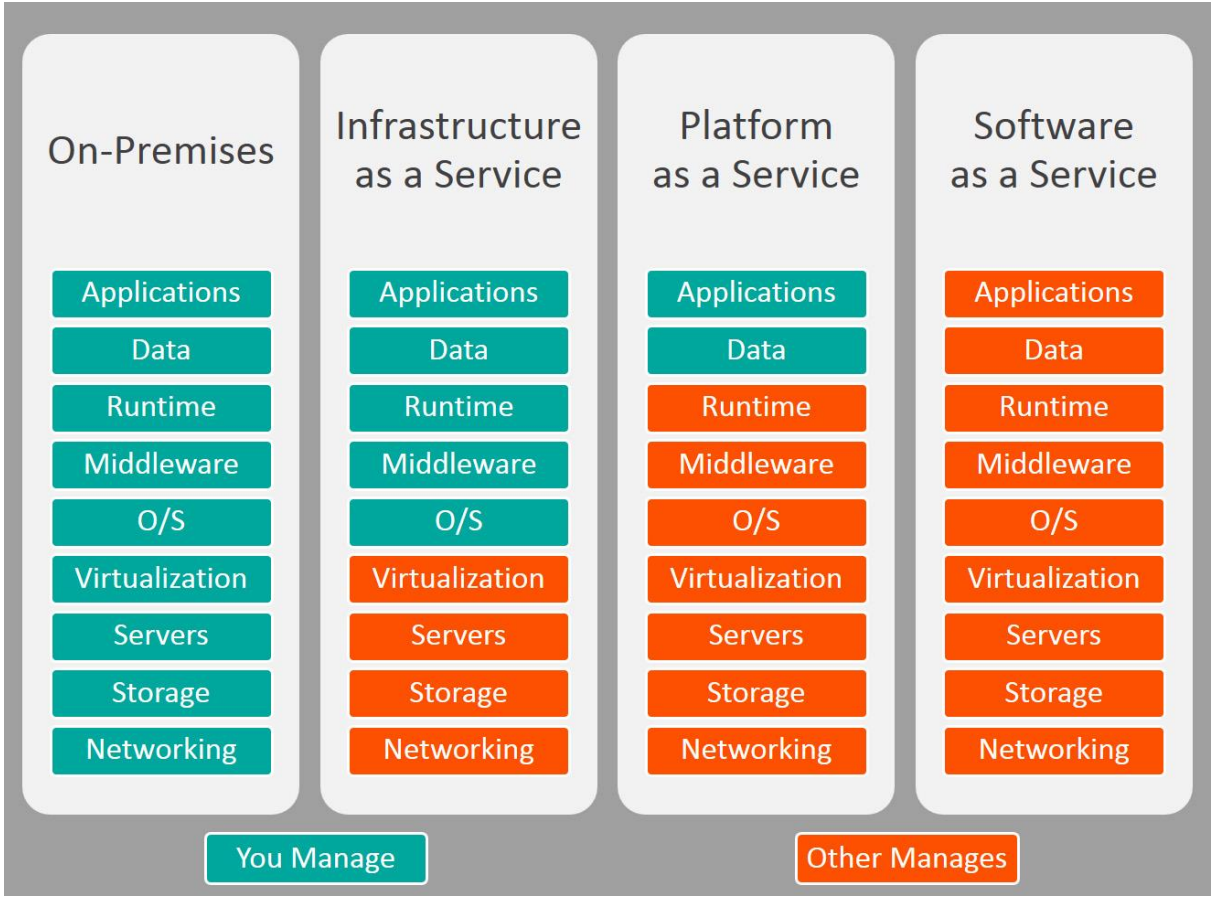
- Gartner defines the Cloud as a style of computing in which scalable and elastic IT-enabled capabilities are delivered as a service using Internet technologies.
    - Public Cloud: Computing, Networking, Server and Storage resources owned and operated by a third party Cloud Service Provider and delivered over the Internet. Public Cloud resources are shared with other organizations and separated into individual tenants.
    - Private Cloud: Computing resources used exclusively by one business or organization. In the Private Cloud services and infrastructures are maintained by your organization. Private Clouds can be physically located in your organizations data center or can be hosted by a third party service provider.
    - Hybrid Cloud: Hybrid Clouds are a mixture on-premise infrastructure, Private Clouds and Public Clouds.

What is the Cloud?

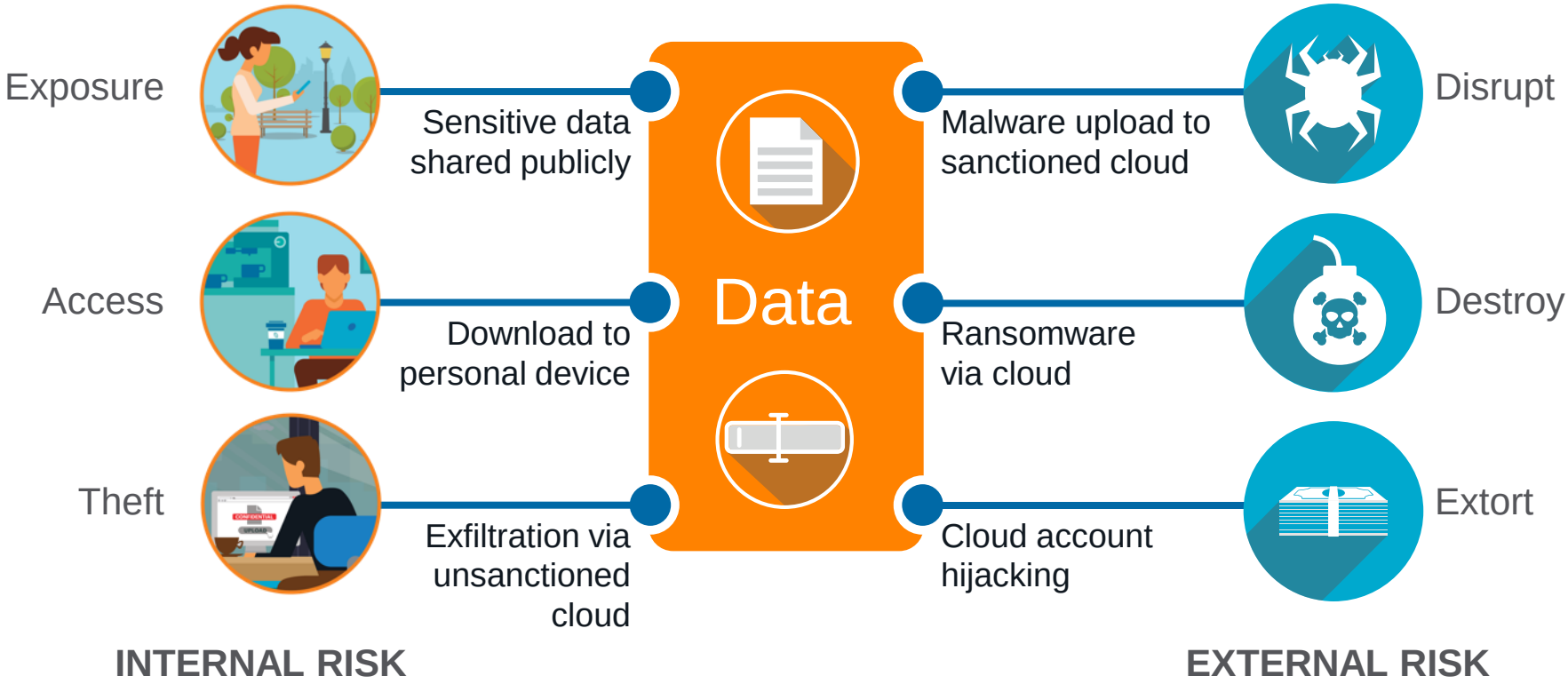


Who in the Organization is Buying and Why?

How is the Cloud delivered: Key differences between Iaas, PaaS and SaaS



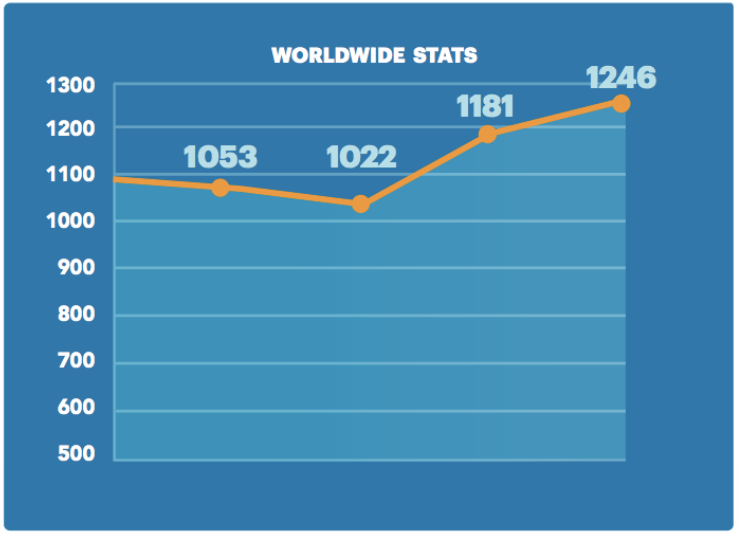
Cloud Security Challenges and Risks



Current Cloud Security Report

Enterprise Use of Cloud Services

On average the number of cloud services in use per enterprise, there was an increase to 1,246 from 1,181 last report.



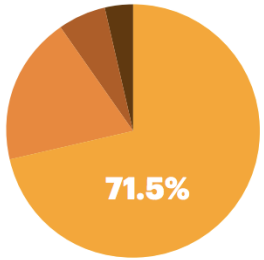
CATEGORY	# PER ENTERPRISE	NOT ENTERPRISE-READY
HR	175	96%
Marketing	170	98%
Collaboration	110	83%
Finance/Accounting	76	94%
CRM	76	93%
IT Service/Application Management	31	93%
Cloud Storage	28	67%
Social	26	92%

Source: Netskope Cloud Security Report, October 2018

Current Cloud Security Report

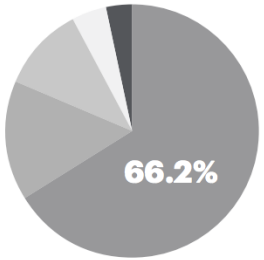
CIS Benchmark Violations for AWS

By category in the CIS benchmark for AWS, the majority of violations are in the Identity and Access Management category at 71.5 percent. Monitoring followed with 19.0 percent, Networking with 5.9 percent, and Logging with 3.6 percent. This may indicate that while many organizations have controls around cloud services and implemented things like multi-factor authentication (MFA) and single sign-on solutions, I/PaaS identity and access policies still need to be set.



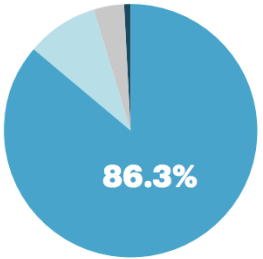
BY CATEGORY

- Identity and Access Management **71.5%**
- Monitoring **19.0%**
- Networking **5.9%**
- Logging **3.6%**



BY RESOURCE

- EC2 **66.2%**
- CloudTrail **15.2%**
- S3 **10.9%**
- IAM **4.5%**
- Other (config., KMS, RD, CloudWatch) **3.2%**



BY SEVERITY

- Critical **86.3%**
- High **9.1%**
- Medium **4.0%**
- Low **0.6%**

Source: Netskope Cloud Security Report, October 2018

THREE QUICK WINS FOR ENTERPRISE IT

1. Place DLP policies and security controls over activities like downloading sensitive information from IaaS solutions to secure increasing use of the public cloud.

2. Assess the security of your IaaS environment continuously against best practices so you can quickly identify and remediate risks and potential vulnerabilities.

3. Consider using the same security profiles, policies, and controls across SaaS, IaaS, and web services to reduce complexity.

Cloud Security Technology Drivers

- Professionals now work from multiple devices in multiple locations
- Instantaneous sharing and collaboration happens through numerous applications
- Firewalls cannot protect data stored throughout various cloud applications
- Traditional security tools cannot provide visibility in the cloud
- Non-enterprise cloud applications are consumed by end users without regard for their risk exposure

Common Use Cases for Cloud Security Technologies

Safely Enable Cloud Apps

Discover Shadow IT

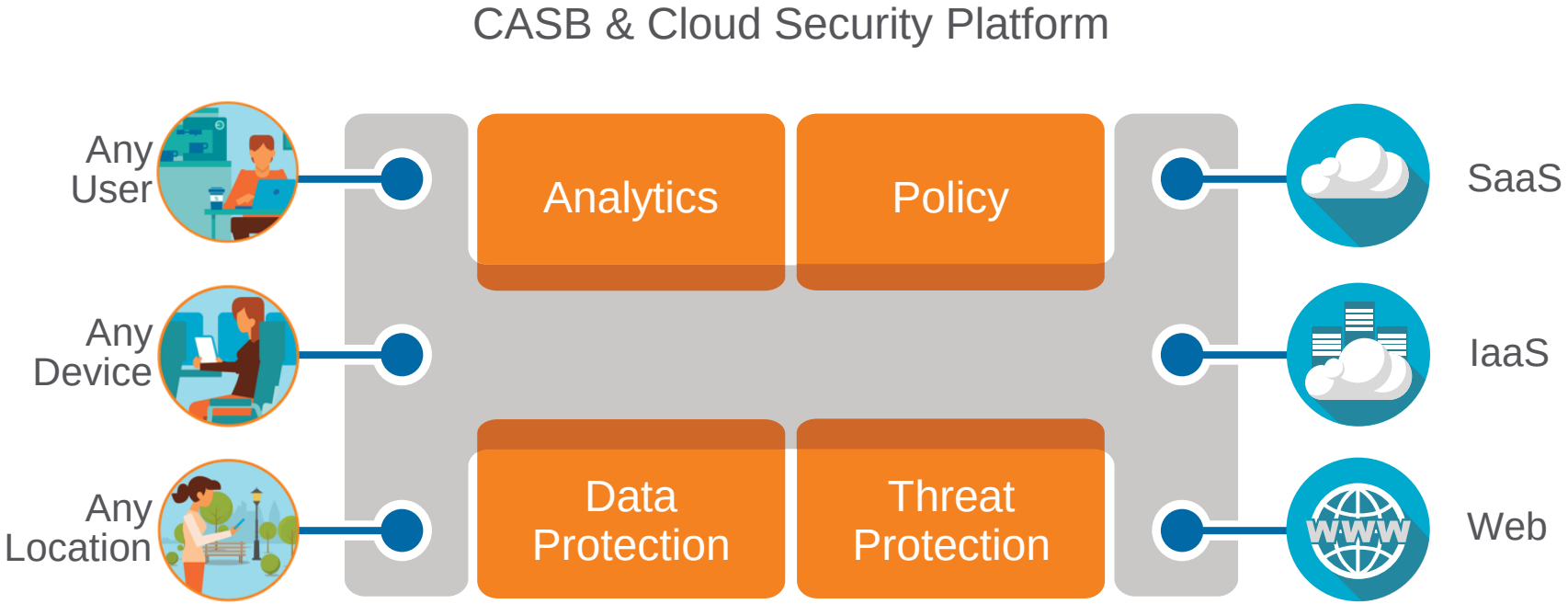
Unified Cloud Policies

Detect Cloud Threats

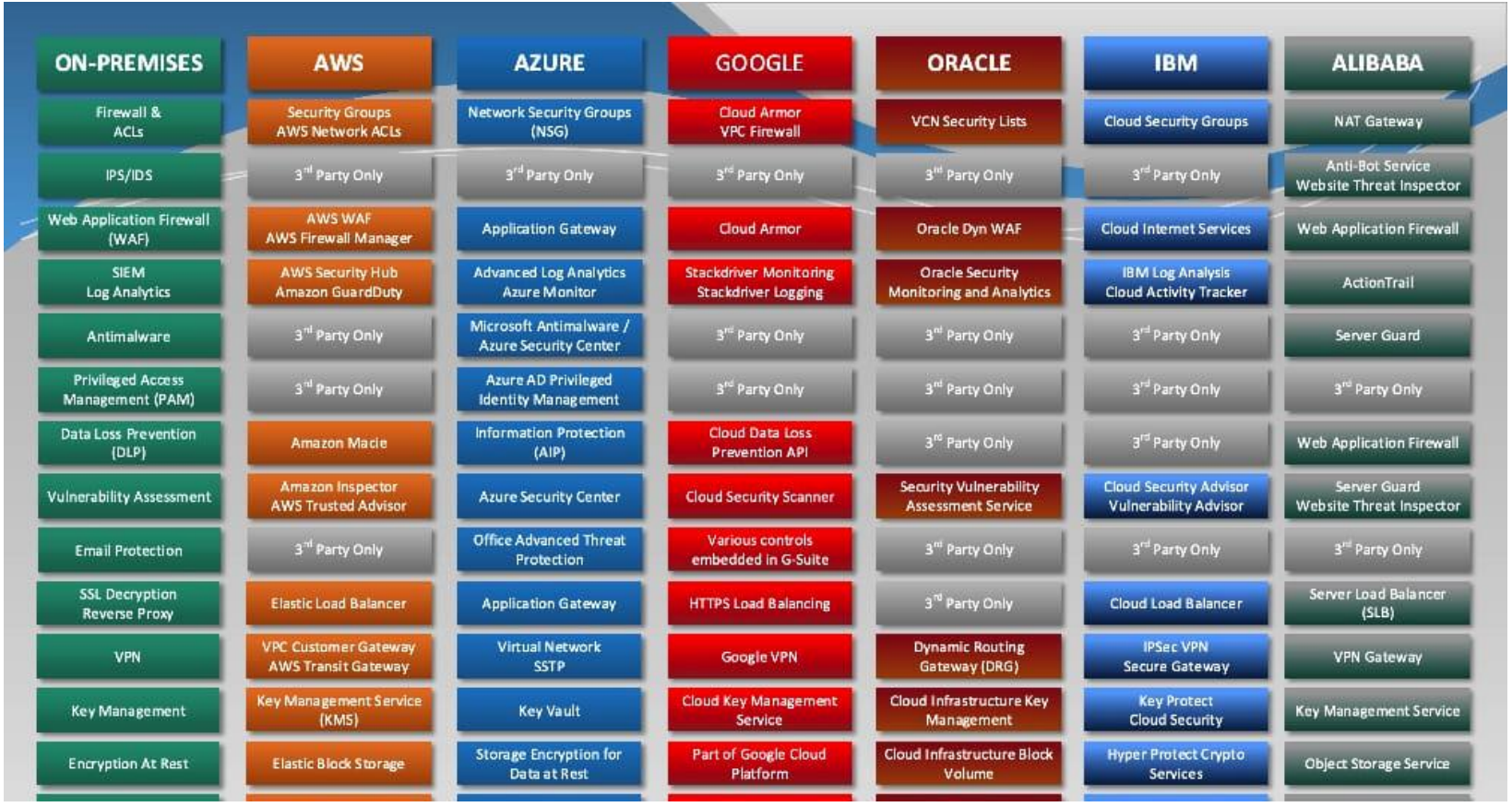
Continuous Security Assessments

Prevent Data Exfiltration

What Technologies Exist to Address Risk?



Mapping of Cloud Security Controls



ON-PREMISES	AWS	AZURE	GOOGLE	ORACLE	IBM	ALIBABA
Firewall & ACLs	Security Groups AWS Network ACLs	Network Security Groups (NSG)	Cloud Armor VPC Firewall	VCN Security Lists	Cloud Security Groups	NAT Gateway
IPS/IDS	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only	Anti-Bot Service Website Threat Inspector
Web Application Firewall (WAF)	AWS WAF AWS Firewall Manager	Application Gateway	Cloud Armor	Oracle Dyn WAF	Cloud Internet Services	Web Application Firewall
SIEM Log Analytics	AWS Security Hub Amazon GuardDuty	Advanced Log Analytics Azure Monitor	Stackdriver Monitoring Stackdriver Logging	Oracle Security Monitoring and Analytics	IBM Log Analysis Cloud Activity Tracker	ActionTrail
Antimalware	3rd Party Only	Microsoft Antimalware / Azure Security Center	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Privileged Access Management (PAM)	3rd Party Only	Azure AD Privileged Identity Management	3rd Party Only	3rd Party Only	3rd Party Only	3rd Party Only
Data Loss Prevention (DLP)	Amazon Macie	Information Protection (AIP)	Cloud Data Loss Prevention API	3rd Party Only	3rd Party Only	Web Application Firewall
Vulnerability Assessment	Amazon Inspector AWS Trusted Advisor	Azure Security Center	Cloud Security Scanner	Security Vulnerability Assessment Service	Cloud Security Advisor Vulnerability Advisor	Server Guard Website Threat Inspector
Email Protection	3rd Party Only	Office Advanced Threat Protection	Various controls embedded in G-Suite	3rd Party Only	3rd Party Only	3rd Party Only
SSL Decryption Reverse Proxy	Elastic Load Balancer	Application Gateway	HTTPS Load Balancing	3rd Party Only	Cloud Load Balancer	Server Load Balancer (SLB)
VPN	VPC Customer Gateway AWS Transit Gateway	Virtual Network SSTP	Google VPN	Dynamic Routing Gateway (DRG)	IPSec VPN Secure Gateway	VPN Gateway
Key Management	Key Management Service (KMS)	Key Vault	Cloud Key Management Service	Cloud Infrastructure Key Management	Key Protect Cloud Security	Key Management Service
Encryption At Rest	Elastic Block Storage	Storage Encryption for Data at Rest	Part of Google Cloud Platform	Cloud Infrastructure Block Volume	Hyper Protect Crypto Services	Object Storage Service

Mapping of Cloud Security Controls cont.

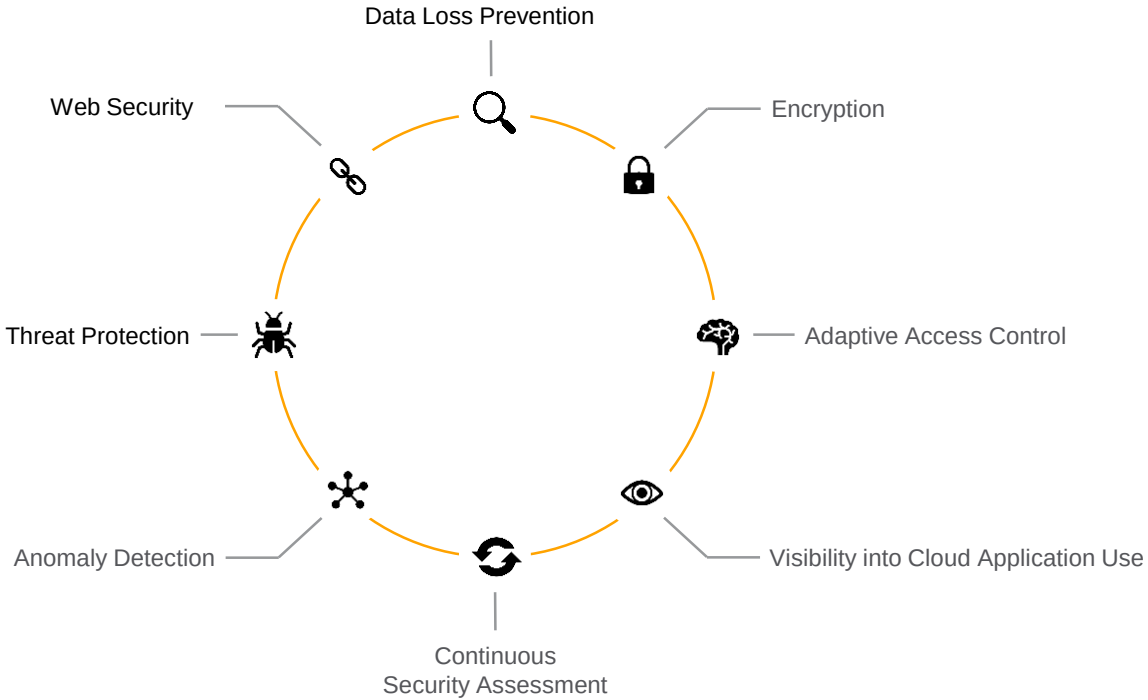
DDoS	AWS Shield	Built-in DDoS defense	Cloud Armor	Built-in DDoS defense	Cloud Internet Services	Anti-DDoS
Identity and Access Management	Identity and Access Management (IAM)	Azure Active Directory	Cloud Identity Cloud IAM	Oracle Cloud Infrastructure IAM	Cloud IAM App ID	Resource Access Management
Multi-Factor Authentication	AWS MFA	Azure Active Directory	Security Key Enforcement	Oracle Cloud Infrastructure IAM	App ID	Resource Access Management
Centralized Logging / Auditing	CloudWatch / S3 bucket	Azure Audit Logs	VPC Flow Logs Access Transparency	Oracle Cloud Infrastructure Audit	Log Analysis with LogDNA	Log Service
Load Balancer	Elastic Load Balancer / CloudFront	Azure Load Balancer	Cloud Load Balancing HTTPS Load Balancing	Cloud Infrastructure Load Balancing	Cloud Load Balancer	Server Load Balancer
LAN	Virtual Private Cloud (VPC)	Virtual Network	Virtual Private Cloud Network (VPC)	Virtual Cloud Network (VCN)	VLANs	Virtual Private Cloud (VPC)
WAN	Direct Connect	ExpressRoute / MPLS	Dedicated Interconnect	FastConnect	Direct Link	VPN Gateway Express Connect
Endpoint Protection	3rd Party Only	Microsoft Defender ATP	3rd Party Only	3rd Party Only	3rd Party Only	Server Guard
Certificate Management	AWS Certificate Manager	3rd Party Only	3rd Party Only	3rd Party Only	Certificate Manager	Cloud SSL Certificates Service
Container Security	Amazon EC2 Container Service (ECS	Azure Container Service (ACS)	Kubernetes Engine	Oracle Container Services	Containers - Trusted Compute	Container Registry
Governance Risk and Compliance Monitoring	AWS CloudTrail AWS Compliance Center	Azure Policy	Cloud Security Command Center	3rd Party Only	3rd Party Only	ActionTrail
Backup and Recovery	AWS Backup Amazon S3 Glacier	Azure Backup Azure Site Recovery	Object Versioning Cloud Storage Nearline	Archive Storage	IBM Cloud Backup	Hybrid Backup Recovery

Mapping of On-Premises Security Controls vs Major Cloud Providers Version 3.2 Feb 2019 © Adrian Grigorof, Marius Mocanu

Source: Peerlyst Post – Adrian Grigorof, February 2019

What Technologies Exist to Address Risk

Technical capabilities needed to address todays risk



Jason Sheffield

Sr. Sales Engineer at Netskope

Questions?

Appendix

- Netskope Cloud Report:

https://resources.netskope.com/cloud-reports/netskope-cloud-report-october-2018

Thank You!